UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/839,551 | 04/19/2001 | Stephen F. Bisbee | 003670-074 | 1293 |

7590 05/21/2003

Michael G. Savage, Esquire
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404

| EXAMINER | |
|---|---|
| FLEURANTIN, JEAN B | |
| ART UNIT | PAPER NUMBER |
| 2172 | 2 |

DATE MAILED: 05/21/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

|  |  |  |  |
|---|---|---|---|
| **Office Action Summary** | **Application No.**<br>09/839,551 | **Applicant(s)**<br>BISBEE ET AL. |  |
|  | **Examiner**<br>Jean B Fleurantin | **Art Unit**<br>2172 |  |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)□ Responsive to communication(s) filed on _____ .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) □ Interview Summary (PTO-413) Paper No(s). _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other:

## DETAILED ACTION

1. Claims 1-41 are presented for examination.

### *Claim Rejections - 35 USC § 102*

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6, 10, 11, 13-17, 29-33 and 37, 38, 40 and 41 are rejected under 35 U.S.C. 102(b) as being anticipated by Karaev et al. (US Pat. No. 5,802,518)("Karaev").

As per claims 1, Karaev teaches a method of enabling access to a resource of a processing system as claimed, comprises the steps of establishing a secure communication session between a user desiring access and a logon component of the processing system (thus, secure system to distribute reports on a timely basis from brokage and investment banking firms to investors and that allows investors to access and query a database of reports located at a remote location; which is readable as establishing a secure communication session between a user desiring access and a logon component of the processing system)(see col. 5, lines 51-54);

Verifying that logon information, provided by the user to the logon component during the secure communication session (thus, when the secure web server 4 receives the request to run 'result.exe', the web server 4 first checks the request to ensure that the Internet browser making the request is authorized to access the web server 4, if the Internet browser is not authorized, the web server 4 prompts the Internet browser to ask the user, via a dialog box, for a valid user ID and password; which is readable as verifying that logon information, provided by the user to the logon component during the secure communication session)(see cols. 26-27, lines 66-14), matches stored information identifying the user to the processing system (thus, a list of the documents that match that search criteria and which the user is authorized to access is provided to the user computer; which is readable as matches stored information identifying the user to the processing system)(see col. 4, lines 11-14);

generating a security context from the logon information and authorization information that is necessary for access to the resource (thus, this user then becomes the designated 'current user of this ID', a new random value for the "mxauth" part of the browser cookie is generated, stored on the web server 4 under this user's ID, and sent back to the Internet browser, so that the Internet browser can send it back next time; which is readable as generating a security context from the logon information and authorization information that is necessary for access to the resource)(see col. 8, lines 50-55);

providing the security context to the user (thus, the web server submits a login request to the CGI program to verify that no other user is using the same ID; which is readable as providing the security context to the user)(see col. 3, lines 60-62); and

sending, by the user to the processing system, the security context and a request for access to the resource (thus, the web server 4 first checks the request to ensure that the Internet browser making the request is authorized to access the web server 4, if the Internet browser is not authorized, the web server 4 prompts the Internet browser to ask the user, via a dialog box, for a valid user ID and password; which is equivalent to sending, by the user to the processing system, the security context and a request for access to the resource)(see col. 27, lines 8-14).

As per claims 2 and 16, Karaev teaches the method as claimed, wherein the resource is at least one of a processor, a program object, and a record of the processing system (see col. 6, lines 52).

As per claim 3, Karaev teaches the method as claimed, wherein the logon component provides a symmetric encryption key to the user in establishing the secure communication session (thus, a secure sign-on procedure is needed that prevents multiple users using the same identification code and allows an authorized user to move to another computer or browser program and still be permitted to access the secure web server; which is equivalent to wherein the logon component provides a symmetric encryption key to the user in establishing the secure communication session)(see col. 2, lines 17-22).

As per claims 4 and 31, Karaev teaches the method as claimed, wherein the logon information includes a password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position (thus, when the user initially accesses the web server, the user is required to provide a user identification code 'ID' and a password, the web server submits a login request to the CGI program to verify that no other user is using the same ID; which is equivalent to wherein the logon information includes a password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position)(see col. 3, lines 58-64).

As per claim 5, Karaev teaches the method as claimed, wherein the logon information is verified by checking for agreement between the stored information identifying the user to the processing system and the password and at least one of a user identifier (see col. 4, lines 11-14), an organization identifier, a sub-organization identifier, a user location, a user role, and a user position provided by the user to the logon component (see col. 3, lines 58-67).

As per claims 6 and 33, Karaev teaches the method as claimed, wherein the security context comprises a plaintext header and an encrypted body, and the plaintext header comprises a security context ID, a key handle, and an algorithm identifier and key size (see col. 2, lines 17-22).

As per claims 10 and 37, Karaev teaches the method as claimed, further comprises the step of determining, by a stateless component of the processing system, based on the security context sent with the request for access by the user, whether access to the requested resource should be granted to the user (thus, this is the first time this user/browser has "logged in", the ‘mxauth’ value in the cookie has not been set, so ‘result.exe’ grants this user access, generates an authorization string for this user, stores the string where it can find it later, and outputs a cookie value to the web server 4 that the server will send back to the Internet browser; which is readable as determining, by a stateless component of the processing system, based on the security context sent with the request for access by the user, whether access to the requested resource should be granted to the user)(see col. 27, lines 43-48).

As per claims 11 and 38, Karaev teaches the method as claimed, wherein the communication device at least partially encrypts the request for access with a symmetric encryption key included in the security context (see col. 6, lines 52).

As per claims 13 and 40, Karaev teaches the method as claimed, wherein the user digitally signs the request for access, the user's digital signature is included with the security context and the request for access sent by the user to the processing system, the user's digital signature is checked by the processing system, and access to the resource is granted only if the user's digital signature is authenticated (see col. 8, lines 26-44).

As per claim 14, the limitations of claim 14 are rejected in the analysis of claim 14, and this claim is rejected on that basis.

As per claim 15, Karaev teaches the method as claimed, further comprises the step, after access to the requested resource is granted, of sending a response to the user that includes a request counter that enables the user to match the response to the request for access (thus, program compares this value to the current authorization code it has stored for this user, and if the two do not match it generates output that tells the user that access has been denied, if the values do match then 'result.exe' proceeds; which is readable as after access to the requested resource is granted, of sending a response to the user that includes a request counter that enables the user to match the response to the request for access)(see col. 32, lines 49-53).

As per claim 17, Karaev teaches the method as claimed, wherein the user sends the request counter and access to the resource is denied if the request counter differs from a predetermined value (see col. 8, lines 29-44).

As per claim 29, in addition to the discussion in claims 1 and 18, teaches an information database that stores information identifying users to the processing system and authorization information that identifies resources accessible to users and that is necessary for access to resources (thus, a list of the documents that match that search criteria and which the user is authorized to access is provided to the user computer; which is readable as an information database that stores information identifying users to the processing system and authorization information that identifies resources accessible to users and that is necessary for access to resources)(see col. 4, lines 11-14); and

a logon component that communicates with the communication device and with the information database, wherein the logon component receives logon information provided by the user during the secure communication session (thus, when the secure web server 4 receives the request to run 'result.exe', the web server 4 first checks the request to ensure that the Internet browser making the request is authorized to access the web server 4, if the Internet browser is not authorized, the web server 4 prompts the Internet browser to ask the user, via a dialog box, for a valid user ID and password; which is readable as a logon component that communicates with the communication device and with the information database, wherein the logon component receives logon information provided by the user during the secure communication session)(see cols. 26-27, lines 66-14).

As per claim 30, Karaev teaches the method as claimed, further comprises a cryptographic accelerator, and wherein the logon component receives a symmetric encryption key from the cryptographic accelerator and provides the symmetric encryption key to the user's communication device (thus, a secure sign-on procedure is needed that prevents multiple users using the same identification code and allows an authorized user to move to another computer or browser program and still be permitted to access the secure web server; which is readable as wherein the logon component receives a symmetric encryption key from the cryptographic accelerator and provides the symmetric encryption key to the user's communication device)(see col. 2, lines 17-22).

As per claim 32, the limitations of claim 32 are rejected in the analysis of claim 1, and this claim is rejected on that basis.

As per claim 41, the limitations of claim 41 are rejected in the analysis of claim 1, and this claim is rejected on that basis.

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7-9, 12, 18-28, 34-36 and 39 are rejected under U.S.C. 103(a) as being unpatentable over Karaev et al. (US Pat. No. 5,802,518) in view of Serbinis et al. (US Pat. No. 6,314,425) ("Karaev"), ("Serbinis").

As per claims 7, 8, 12, 22, 24, 34, 35 and 39, Karaev teaches the claimed subject matter except the claimed wherein a hash value is computed over the request for access, the hash value is included with the security context and the request for access sent by the user to the processing system, the integrity of the request for access is checked based on the hash value, and access is granted only if the integrity of the hash value is verified. However, Serbinis teaches using a one-way hashing algorithm, adding a timestamp, and then signing the resulting data with a private key, (see col. 9, lines 38-40). Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Karaev and Serbinis with wherein a hash value is computed over the request for access. This modification would allow the teachings of Karaev and Serbinis to provide access control protocol (see col. 3, lines 2-3).

As per claims 9 and 36, Karaev teaches the method as claimed, wherein the encrypted body includes the expiration time and access to the resource is denied if the expiration time differs from a selected time (thus, prevent concurrent use of a user's identification code and password 'e.g., to prevent the user from distributing the user's identification code and password for use by others' when a user initially accesses a web server, the web server, using current password technology, can prevent other access with that identification code for a predetermined period of time; however, if the user moves to another computer or browser program, then the authorized user will be prevented from accessing the web server from the new computer or browser program; which is readable as wherein the encrypted body includes the expiration time and access to the resource is denied if the expiration time differs from a selected time)(see col. 2, lines 7-16).

As per claim 18, in addition to the discussion in claim 1, Karaev further teaches determining, by a stateless component of the processing system, based on the security context sent with the request for access by the user, whether access to the requested resource should be granted to the user (thus, this is the first time this user/browser has 'logged in', the 'mxauth' value in the cookie has not been set, so 'result.exe' grants this user access, generates an authorization string for this user, stores the string where it can find it later, and outputs a cookie value to the web server 4 that the server will send back to the Internet browser; which is readable as determining, by a stateless component of the processing system, based on the security context sent with the request for access by the user, whether access to the requested resource should be granted to the user)(see col. 27, lines 43-48);

wherein the security context comprises a plaintext header and an encrypted body; the plaintext header comprises a security context 1D, a key handle, and an algorithm identifier and key size (thus, the web server submits a login request to the CGI program to verify that no other user is using the same ID; which is readable as a security context 1D, a key handle, and an algorithm identifier and key size)(see col. 3, lines 60-62); and the encrypted body comprises at least one of a user identifier, an organization identifier, access information (see col. 3, lines 58-62), an expiration time, public key information, symmetric key information, (thus, prevent concurrent use of a user's identification code and password 'e.g., to prevent the user from distributing the user's identification code and password for use by others' when a user initially accesses a web server, the web server, using current password technology, can prevent other access with that identification code for a predetermined period of time; however, if the user moves to another computer or browser program, then the authorized user will be prevented from accessing the web server from the new computer or browser program; which is readable as an expiration time, public key information, symmetric key information, and a hash) (see col. 2, lines 7-16). But, Karaev does not explicitly indicate a hash. However, Serbinis implicitly indicates using a one-way hashing algorithm, adding a timestamp, and then signing the resulting data with a private key, (see col. 9, lines 38-40). Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Karaev and Serbinis with a hash. This modification would allow the teachings of Karaev and Serbinis to provide access control protocol (see col. 3, lines 2-3).

As per claim 19, the limitations of claim 19 are rejected in the analysis of claim 3, and this claim is rejected on that basis.

As per claim 20, the limitations of claim 20 are rejected in the analysis of claim 4, and this claim is rejected on that basis.

As per claim 21, the limitations of claim 21 are rejected in the analysis of claim 5, and this claim is rejected on that basis.

As per claim 23, the limitations of claim 23 are rejected in the analysis of claim 9, and this claim is rejected on that basis.

As per claim 25, the limitations of claim 25 are rejected in the analysis of claim 13, and this claim is rejected on that basis.

As per claim 26, Karaev teaches the method as claimed, further comprises the step, after access to the requested resource is granted, of sending a response to the user that includes a request counter that enables the user to match the response to the request for access (thus, program compares this value to the current authorization code it has stored for this user, and if the two do not match it generates output that tells the user that access has been denied, if the values do match then 'result.exe' proceeds; which is readable as after access to the requested resource is granted, of sending a response to the user that includes a request counter that enables the user to match the response to the request for access)(see col. 32, lines 49-53).

As per claim 27, the limitations of claim 27 are rejected in the analysis of claim 1, and this claim is rejected on that basis.

As per claim 28, the limitations of claim 28 are rejected in the analysis of claim 17, and this claim is rejected on that basis.

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Kitain et al. US Patent Number 5,864,871 relates to computer-based system.

***Conclusion***

5. Any inquiry concerning this communication from examiner should be directed to Jean Bolte Fleurantin at (703) 308-6718. The examiner can normally be reached on Monday through Friday from 7:30 A.M. to 6:00 P.M.

If any attempt to reach the examiner by telephone is unsuccessful, the examiner's supervisor, Mrs. KIM VU can be reached at **(703) 305-8449.** The FAX phone numbers for the Group 2100 Customer Service Center are: ***After Final*** **(703) 746-7238,** ***Official*** **(703) 746-7239,** and ***Non-Official (703) 746-7240***. NOTE: Documents transmitted by facsimile will be entered as official documents on the file wrapper unless clearly marked "***DRAFT***".

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group 2100 Customer Service Center receptionist whose telephone numbers are **(703) 306-5631, (703) 306-5632, (703) 306-5633**.

Jean Bolte Fleurantin

2003-05-12

JBF/

JEAN M. CORRIELUS
PRIMARY EXAMINER